Welcome

- Security
- Privacy
- Sustainability

Agenda

11:00   Introductions, Who You Are? Why do you care?
11:30   Overview of Online Trust Audit - IoT Segment performance
11:45   IoT Security research - Geoff Noakes - Symantec
12:00   Lunch - Glenn Derene, Editor Consumer Reports Magazine
1:00    Review of draft framework / Breakouts
4:00    Breakouts report back to group
5:00    Considerations of a possible seal / certification program
5:45    Wrap Up & Reception

Reminders

- Chatham House Rule
- Introductions
  - Who are You & Why do You Care?
- Listen, Learn + Collaboration = Innovation
OTA

501c3 charitable organization with a mission to enhance online trust, while promoting innovation and the vitality of the internet.

- Goal to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.
- OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.

Focused On Collaboration
What Do We Want to Achieve Today

- Review framework progress to date
- How can we collaborate with others?
- Critique, validate and prioritize criteria
  - What are we missing?
  - How can it be validated and measured
  - Is it applicable for all device categories?

Working Group Goals

1. Provide guidance to manufacturers and developers to help reduce attack surface and vulnerabilities, and adopt responsible privacy and data stewardship practices.
2. Drive the adoption of best practices; embracing “privacy and security by design”, as a model for the development of a voluntary, yet enforceable code of conduct.
3. Provide positive affirmation and recognition to companies, products, and retailers who embrace the code of conduct and meet minimum standards.
4. Provide retailers/commerce sites criteria to aid in their product merchandising and promotion decisions.
5. Where possible, apply existing standards from NIST, NTIA, ISO and other industry working groups.
7. Evaluate and identify gating issues and considerations which may lead to the development of a seal or certification program which could become an incentive to adopt best practices.

Unique IoT Challenges

1. Highly personal, dynamic, persistent collection and transfer of data.
2. Reliance on a combination of devices, apps, platforms and cloud services.
3. Multiple data flows.
4. Multiple touch points and disclosures.
5. Sustainability / Lifecycle issues.
7. Non-traditional market players and rush to market.
Concerns

1. Unknown and future secondary data usages; unintended consequences
2. Unique devices which impact disclosures
3. Compatibility; ability to roll back updates and patches?
4. Impact to core functionality of the product purchased; changes in policies
5. Product warranty/support, beyond traditional guarantees (aka auto recalls vs repairs)
6. Reliance on installers/third parties. What are they doing and setting on behalf of the consumer?
7. Similarity to PCI. If you handle, touch, store or transfer cc info you must be compliant
8. AV for IoT? They will be hacked and compromised!
9. Consent; does it transfer with home ownership?
10. What happens to my data? Portability, compatibility with other devices. Can I retract my data?

Multi-Dimension Landscape & Issues

• Data Security
• Privacy
• Sustainability
  ▪ Lifecycle issues
  ▪ Supportability
  ▪ Data retention/ownership
• Data In use, transit & rest

Security – Top 10 OWASP

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security
Working Group Review & Priorities

What Consumers Need To Know

1. Does my device / application have a posted privacy policy which respects my data and privacy?
2. Can I opt-in or opt-out and what will the impact be to the product functionality?
3. Does the manufacturer and app developer follow a Security Development Lifecycle (SDL)?
4. Is my data protected at rest and in transit?
5. Does my device have a published support policy including end of life?
6. How will my device be upgraded to address security vulnerabilities? How will I be notified?
7. How can my data be deleted if the device is lost, stolen or sold?
8. How can I compare security and privacy practices as part of my purchase decision?
9. Does the manufacturer (and retailers) share or monetize my data?
10. What is the risk my personal data could be re-identified?

Online Trust Audit & Honor Roll
Honor Roll Overview

- Analysis of ~1,000 websites
  - FDIC Banking 100
  - Internet Retailer 500
  - Top 50 Social
  - Top 50 News/Media
  - Top 50 Federal Gov’t
  - OTA Members
  - IoT 50 (Home automation, Wearables)

- Scoring:
  - Up to 100 points in each category
  - Bonus points for emerging practices
  - Penalty points for
    - Data loss incident
    - Fines/settlement
  - Honor Roll = 80% of total points, 55% or better in each category

Privacy

- Base points
  - Privacy policy
  - Third-party trackers on site

- Bonus points
  - Layered privacy policies
  - Bilingual policies
  - Use of icons
  - Do Not Track status, policy
  - Tag mgmt., or privacy solution

- Penalty points
  - WHOIS (if Private vs Public)
  - Data Breach Incidents
  - FTC / State Settlements

Consumer & Brand Protection

- Base points
  - Email authentication
    - SPF and DKIM at top-level and subdomains
  - DMARC record and policy

- Bonus points
  - TLS for email
  - DMARC reject policy

- Penalty points
  - Domain locking (not locked)

- Can the app or web site be spoofed fooling a consumer to open or download an update, open an attachment or simply open an email with a drive-by exploit?
- Does the site or app exercise best practice to help prevent brand jacking and domain abuse?
Infrastructure Security

- Base points
  - Server & SSL implementation
- Bonus points
  - EV SSL
  - AOSSSL
  - DNSSEC
- Penalty points
  - XSS / iFrame vulnerabilities
  - Malware
  - Malicious links
  - Bot risk

Overall Achievement

Review By Segment
Top of The Class

#1 of all Online Retailers

Ranked #1 across all sectors

IoT - Highlights

Who Made The Grade for IoT?
Range & Median

IoT Key Metrics

Privacy Scoring
Case Study – IoT Security

Geoffrey Noakes
Senior Director, Business Development
geoffrey_noakes@symantec.com
+1-415-370-5980

Many consumer products are now Internet-connected

© 2015. All rights reserved. Online Trust Alliance (OTA)
Remember the fridge that sends out spam?

The IoT device was behind a NAT router
- A typical PC, infected with malware, was sending out spam
- The fridge was behind the same NAT router
- It is technically possible to have fridges send spam

Let's consider some "health wearables"
Where are the risks?

- IoT devices are Internet-connected and have all the same risks as typical PCs and smartphones

Symantec analysis of health apps

- We analysed the top 100 free health applications

Who do health apps share data with?

- Each of these vendors could share your data again

© 2015. All rights reserved. Online Trust Alliance (OTA)
Your data is already being analysed

Jawbone: Who’s asleep during San Francisco earthquake 2014?

The IoT is raising the interest of attackers

- Infects routers
- PHP vulnerabilities
- Default passwords
- MiWi implementations

Many proof of concepts around, but attackers are currently finding it difficult to make the activity profitable

A very real example: Smart hub devices

- Unsigned firmware update (MITM attack possible)
- Passwords sent in clear text (no SSL encryption)
- 4-digit PIN code in the cloud enforced (blind SQL injection)
Common issues we found when analysing devices

- Weak authentication (or no password at all)
- No encryption
- Prone to web vulnerabilities (66% had OWASP vulnerabilities)
- Privacy concerns
- Firmware updates: either missing or unsigned
- Full trust to any local device
- Insufficient security configurability
- Simple physical attacks are possible
In the Privacy of Your Own Home
(June 2015 Issue)

Even Mr. Coffee is watching you

What makes an object “smart”?
- Sensors
- Internet connectivity
- A degree of autonomy
- Can be part of an ecosystem
Which of these is an IoT device?

- Computer?
- Smartphone?
- Navigation Device?
- Game Console?
- Bluetooth Speaker?
- Amazon Echo?

The landscape of IoT devices

How big is the Internet of Things?
- FTC report estimates 25 billion connected devices this year.
- By 2020, that number is expected to grow to 50 billion.

What kinds of data are collected?
- Many IoT devices are meant to be integrated into the intimate spaces of our homes and lives.
- The data collection becomes a passive by-product of our interaction with the device.

© 2015. All rights reserved. Online Trust Alliance (OTA)
The creepiness factor.

• When consumers don’t know what their devices are doing, they freak out.

• If data collection isn’t made explicit, people jump to the worst possible conclusions about motive.

The creepiness factor.

• Samsung was caught off guard by public reaction, and had to respond to public outcry.

Hidden in the fine print.

• The uproar hid a more disturbing trend in the industry.

• Many smart TVs are collecting data on everything you watch and sending it to third parties.
Where, precisely, is your data going?
- We investigated the data stream from smart TVs
- Third-party companies most consumers have never heard of, such as Cognitive Networks and Enswers

What does consent look like?
- People don’t read privacy policies
- It’s even more onerous to expect them to do so for an appliance

What’s the potential harm?
- In 2014, hackers took over baby monitors and broadcast at them
- We’ve discovered websites that search unprotected webcams—some in people’s homes
Where is this going?
- Amazon's Dash program lets participants install buttons to automatically order brand-name supplies.

How much information do we owe companies?
- Diagnostics
- Usage data
- Firmware updates
- Interactions with other appliances
- Health-related data

What is Consumer Reports' role?
Investigating partnerships with:
- NYU Polytechnic
- Georgetown Law Center for Privacy and Technology
- Carnegie Mellon University CHIPS/CUPS Lab
Multi-Dimension Landscape & Issues

- Data Security
- Privacy
- Sustainability
  - Lifecycle issues
  - Supportability
  - Data retention / ownership
- Data in use, transit & rest

Working Group Update

- Security
- Sustainability
- Privacy Team Joanne
- Privacy Team Thea

Feedback

- Scope Changes
- Areas on consensus
- Open for debate
- Key Priorities
Seal Program Discussion
Program Considerations

ITWG Workshop
June 16, 2015

Panelists

• Neal Feather
  ▪ President, SiteLock

• Joanne Furtsch
  ▪ Director of Product Policy, TRUSTe

Starts with clear, consistent, verifiable criteria

• Program scope definition
  ▪ What do the criteria apply to?
  ▪ Are there multiple levels of certification or different criteria or programs based on data type or role in the ecosystem?

• Certification model
  ▪ Third-party validation or self-attested
  ▪ Review/testing methodologies
  ▪ Automated and manual testing approaches
  ▪ Device version changes

• Criteria validation among industry stakeholders
  ▪ Device manufacturers, Industry trade organizations, Retailers, Consumers, Regulators

• Criteria adoption and program brand recognition building
Managing use of the Seal

- Seal usage guidelines
  - Where is the seal allowed to be displayed?
- Process to issue the seal
- Process to revoke seals
- Dispute process (manufacturer and consumer)
  - Define scope of dispute resolution
  - Frequency of verification of criteria/renewal
- Survival
  - Controlling entity changes due to acquisition or merger
- Bankruptcy

Trust in the Seal

- Seals must be dynamic
  - QR Code, RFID, hosted seal, or seal image
- Steps to prevent counterfeiting
  - Trademark protections
- Level of certification must be clear from seal
- Information on certification status accessible from the seal
  - Validation page
- Single, simple source with trusted chain of control for authenticity
- Ongoing monitoring of program compliance and proper seal usage

Generalized certification process

- Monitor
  - Review of device and related Privacy Policies
- Analyze
  - Gap analysis of data collection to certification criteria
  - Findings report
- Award
  - Activate seals and customer validation pages
- Remedy
  - Remediate identified gaps
- Advise
  - Remedy identified gaps

© 2015. All rights reserved. Online Trust Alliance (OTA)
Certification is a business

Next Steps

• OTA IoT Initiative https://otalliance.org/IoT
  • Send feedback to discussion draft by June 26th – craigs@otalliance.org
  • July 1 – Member Working Group Call
  • Aug TBD
  • Nov 16 – DC Dinner with FTC / IoT Caucus
  • Nov 17 – Working meeting – DC